

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION**

**IN THE MATTER OF THE SEARCH OF
ANY DIGITAL DEVICES FOUND ON
COREY GIRMAN AT THE
CHARLOTTE/DOUGLAS
INTERNATIONAL AIRPORT UNDER
RULE 41**

Case No. 3:20-mj-7

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE**

I, Aaron J. Seres, being duly sworn, declare and state as follows:

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation (FBI), and have been since 2004, approximately 15 years. I have been assigned to the investigation of criminal matters for a majority of my service time, including crimes involving the use of computers. Upon entry to the FBI, your Affiant received 18 weeks of specialized training as a Special Agent which included thorough instruction regarding various criminal statutes and elements. In addition to the 18 weeks of initial training, throughout my career as a Special Agent, I have attended more than 1,200 hours of additional conferences, training courses and seminars, to include training specific to conducting cyber-crime investigations. In addition to working as a field agent, I have also held supervisory positions in the FBI's Criminal Investigative Division where I was responsible for the FBI's internet fraud program oversight amongst many other program responsibilities, and was a voting member in reviewing and approving undercover investigations to include investigations of crimes against children. As part of my current duties, I

investigate violations of federal law, including the online exploitation of children, particularly in relation to violations of Title 18, United States Code (USC), Sections 2251, 2252 and 2252A which criminalize, among other things, the production, advertisement, possession, receipt, accessing with intent to view and transportation of child pornography. I have gained experience in the conduct of such investigations through training in seminars, classes, and work related to these types of investigations.

2. As a federal agent, I am authorized to investigate violations of United States law, and, as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

PURPOSE OF AFFIDAVIT

3. This Affidavit is made in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure authorizing the search of the property, specifically any digital devices ("Devices") found on Corey GIRMAN ("GIRMAN") at the Charlotte/Douglas International Airport on January 11, 2020, and the examination and extraction from that property of electronically stored information as described in Attachment B.

4. The facts and information contained in this Affidavit are based on my training and experience, information obtained from federal and/or state law enforcement officers, and relevant documents and/or computer files. This Affidavit contains only information necessary to show that there is sufficient probable cause for the requested warrant and does not set forth every fact known to the government.

5. Based on my training and experience, and the facts stated herein, I respectfully submit that there is probable cause to believe that violations of 18 US Code § 2252(a)(2)

Conspiracy to Distribute and Receive Child Pornography and 18 US Code § 2251(d)(1)(A) Notice Seeking to Receive Child Pornography have been committed. There is also reason to believe that the Devices will contain evidence of violations of 18 US Code §2252(a)(2) Transportation of Child Pornography. the Furthermore, there is probable cause to search the Devices described in Attachment A for evidence, instrumentalities, contraband, or fruits of this crime, and for records to help identify and locate the perpetrator of this crime, as further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(a), (b)(1)(A), (c)(1)(A). Furthermore, the item to be searched and seized will be in this District at the time this warrant is executed.

STATEMENT OF PROBABLE CAUSE

7. In 2017, the Salt Lake City Division of the FBI conducted an investigation on Kik user “KitB10”, identified as Daxton T.B. Hansen.¹ The FBI discovered that Hansen used his Kik account to share, post, and trade images of child pornography. In April 2017, the Salt Lake City

¹ Kik Messenger is a chat application for mobile devices in which users can send text messages, pictures, and videos to other users. Users can communicate directly with an individual or with multiple users in a group chat. When signing up for a Kik account, a user supplies an email address (which does not have to be verified), a unique username, and a display name that is seen when chatting with others. Kik conversations, and uploaded pictures/videos exchanged during the chats, can be forensically extracted or video recorded from a mobile device. When reviewing an extracted Kik chat, an investigator will typically see a screenshot from that video, or an icon indicative of a video file.

Division conducted a search warrant on Hansen's residence and seized multiple electronic devices, several of which contained possible child pornography. During an interview of Hansen, Hansen admitted to viewing and sharing child pornography for approximately two years via Kik, using the "KitB10" profile. Additionally, the FBI learned that Hansen was communicating with hundreds of users on Kik, and was the Administrator of multiple child pornography groups on Kik, in which the members traded nude images of minors and videos of young prepubescent boys engaged in sexually explicit conduct. Hansen, and the other Kik users he communicated with, frequently traded child pornography via Dropbox, pCloud, and other cloud based storage applications. Hansen provided consent for the FBI to assume his Kik identity in an undercover capacity. Based on Hansen's consent, an undercover (UC) agent in the Salt Lake City Division assumed Hansen's "KitB10" Kik account and conducted several undercover sessions during April and May 2017.

8. On or about April 30, 2017, the Kik user "cjbwdc," with display name "Trading Dropbox," joined a Kik group called "Boys links Only! Send On Entry Or be kicked." Hansen was one of the administrators² of this Kik group. Shortly after joining, one of the other administrators told the user "cjbwdc" that the account needed to "send or leave," which based upon training and experience law enforcement has learned usually means that a user must post child pornography in order to remain an active member of the group. User "cjbwdc" posted, "young right," and an administrator responded "boys only." On April 30, 2017, at approximately

² An administrator is a member of a Kik group who has the authority to invite new members to and ban members from a group as well as to set the rules for the group.

10:07 p.m., the account “cjbwdc” posted a Dropbox link to the Kik group. The content of this link is unknown, because the UC was not able to obtain the content at the time the UC observed the link and the content is no longer available.

9. Comments made in the group were indicative of members seeking links containing child pornography, for example: “I’ll send but I need no limit young boys incest brothers I love it all just under 5 please,” “any one have links under 10 incest brothers daddy I love it all,” “Im looking for young boys fucks older girls,” and “anyone got young boys having sex with girls.”

10. There were five additional UC sessions conducted in May 2017 during which “cjbwdc” was still a member of this Kik group. During these sessions, other Dropbox, mega, and pCloud links were posted to the group, some of which included descriptions such as “preteen,” “XXX,” “Gurlz,” and “boyz.” The UC accessed, downloaded and viewed files containing child pornography from these links that would have been available to all members of the Kik group, including “cjbwdc.” The following are examples of what was downloaded from the available links:

- a. The file titled “9(1) copy.mp4” is a 4 minute 37 second video that depicts what appears to be a prepubescent boy, fully nude, in the shower with an adult male, of which only his penis can be seen. The child performs oral sex on the adult male penis, licks the penis, and masturbates the penis. The adult male masturbates himself with his penis pressed against the child’s mouth. The adult male then ejaculates near the child’s mouth.
- b. The file titled “NV-0139 GAY PRETEEN KDV 06.mpg” is a 54 minute

one second video depicting what appears to be two prepubescent clothed male children sitting on a bed. During the video the children undress, masturbate each other, masturbate themselves, and have oral and anal sex with each other.

- c. The file titled "Night25.avi" is a 14 minute 18 second video that depicts a prepubescent male child, fully nude, on top of a naked adult man, who appears to be lying on bed. The child masturbates the man's penis and performs oral sex on the adult. The video then appears to show the adult man's penis being inserted into the child's anus, while the child holds the penis. The adult man then masturbates the prepubescent child's penis. The man has anal sex with the child while masturbating the child. The video has the words "AaronGermany Production" across the bottom the entire time.

11. Around May 22, 2017, the UC was removed from the group, presumably for failing to distribute child pornography to the other members of the group.

12. From approximately October 12, 2017 to October 19, 2017, the UC engaged "cjbwdc" directly, asking "Hey anything new to trade?" and stating, "I have links." "cjbwdc" responded with, "send young." The UC asked, "what age do u have? or do you want?" To which "cjbwdc" responded, "Under 12." The UC made several posts after this which were not answered by "cjbwdc."

13. A subpoena was issued to Kik for information on the user account "cjbwdc" and the results, dated July 17, 2017, revealed a confirmed email address of cjbwdc11@gmail.com

and an account registration date of June 4, 2015. The results also indicated that, as of July 12, 2017, an iPhone was being utilized to access Kik. Additionally, Internet Protocol (IP) Address records from June 19, 2017 to July 12, 2017 were provided and show that IP address 71.62.172.90 was the only IP address being used during this time frame. A subpoena was subsequently issued to Comcast for IP address 71.62.172.90. The results, dated August 14, 2017, reveal the subscriber of the account associated with IP address 71.62.172.90 at the time it was used to access the "cjbwdc" Kik account to be Will Smith("Smith"), with a service address at 20362 Mount Pleasant Ter, Ashburn VA 20147, and using telephone number 814-688-6065. The records also reveal that this IP was assigned to Smith between March 2, 2017 and August 14, 2017, which was the date range of the subpoena returns. This IP assignment date range covers the time period when the initial UC sessions were conducted.

14. A subpoena was issued to Google for the cjbwdc11@gmail.com account. The results, dated November 1, 2017, revealed that the account was created on August 10, 2015 by an individual listed as CJ Beed. There were no IP logs associated with this account.

15. On January 9, 2018, a subpoena was issued to Kik for the account with user name "cjbwdc," and the results, dated January 10, 2018, revealed that the account was still active and that an iPhone was still being utilized to access Kik. Additionally, there were several IP address associated with this account from December 11, 2017 to January 10, 2018, the date range provided pursuant to the subpoena. All but two of the IP addresses were Verizon Wireless natting IP addresses, and a subpoena was issued for those IP addresses. An examination of the information provided by Verizon identified the target telephone number that utilized these IP addresses as 214-949-0996. The subscriber was identified as Raventek Solution Partners, with

an address of 13900 Lincoln Park Drive, Ste. 150, Herndon, VA 20171. The account associated with this telephone number had been active since May 13, 2017, and it was currently active as of the date of the subpoena. The IMEI³ for the telephone was provided as 355342081245513.⁴

16. An additional IP address included in the Kik subpoena response, 73.163.34.138, was utilized to access the “cjbwdc” Kik account on December 30, 2017 and January 2, 2018. That IP address resolved to Comcast, and a subpoena was issued for subscriber information on the dates and times it was used to access the Kik account. Records provided by Comcast indicated that at the dates and times it was used to access the “cjbwdc” Kik account, the subscriber was listed as Jeffrey Marn, with a service address of 3415 Brown St, NW #A, Washington, DC 20010.

17. In February 2018, a 2703(d) Court Order was issued to Apple, Inc. for information pertaining to telephone number 214-949-0996. The return information provided by Apple, Inc. revealed that the Apple, Inc. customer was Corey Girman (“GIRMAN”), with an address of 3425 Porter St., NW, Washington, DC and email address coreymgirman@yahoo.com.

18. In August 2018, an open source query for “cjbwdc” was conducted. Dozens of postings were located on the public website “Sexting on Kik” (www.sextingonkk.com) beginning in February 2016 through October 2018 by user “Cjbusa” who, in multiple posts, indicated he could be reached via Kik user accounts “cjbwdc” or chelsbbbb.” The “Sexting on

⁴ An International Mobile Equipment Identity Number, or IMEI, is a unique identifying number assigned to a mobile device, similar to a serial number.

Kik” profile username, “Cjbusa,” was created in February 2016 with the most recent posting in October 2018. The user “Cjbusa” had approximately 75 posts on the account related to the trading of Dropbox links containing child pornography. Examples of these posts are as follows:

- a. June 27, 2016 titled “Dropboxtrade Group.” This post read, “if you want to trade young, send a link to start. If you want to be added to the group, send two young links and I will add you, we trade daily. Kik chelsbbbbb or cjbwdc.”
- b. May 12, 2018 titled “Young Dropbox Group.” This post reads, “Have an active young Dropbox trading group. Send 2 links and I’ll add you to the group. Must be young. Under 15. Kik: chelsbbbbb.”
- c. September 5, 2018 titled “Young trading group.” This post reads, “Young links (Dropbox/mega) only, send 2 links and I’ll add you to the group :) we are active, please be active too. And be girls or boys :) Young, young bjs, young lesbian, young fucking :P Kik: chelsbbbbb.” This text was followed by numerous smiley face emojis.

19. A Grand Jury subpoena was issued to Kik for user name “chelsbbb” and the results, dated August 15, 2018, revealed the account user’s name to be “C B”, with an unconfirmed email address chelsbbbbb@gmail.com. The account registration date was January 21, 2016, and an iPhone was being utilized to access Kik. Additionally, there were IP address associated with this account from July 19, 2018 to August 9, 2018. The most recent IP address was 73.163.34.138. A Grand Jury subpoena was issued to Comcast for this IP address during the

time frame of the IP logins. The results provided by Comcast, dated August 22, 2018, revealed that the subscriber was still Jeffrey Marn, with the listed address 3415 Brown St, NW #A, Washington, DC 20010.

20. Open source and law enforcement sensitive information available in September, 2018 revealed Corey GIRMAN resided at 3415 Brown St., NW, Washington, DC as of February 2018. Information provided by the United States Postal Inspection Service in September, 2018 indicated that GIRMAN was currently receiving mail at this address, having lived there since December 2017. Additionally, a professional networking profile was located that indicated that GIRMAN worked as a Systems Engineer at Raventek Business Group.

21. On October 15, 2018, a federal search warrant was authorized by Hon. Deborah A. Robinson, United States Magistrate Judge for the District of Columbia for the premises located at 3415 Brown St., NW #A, Washington, DC 20010. On October 23, 2018 that warrant was executed and several electronic devices were seized. In addition to GIRMAN, three other individuals lived at the residence. All residents, including GIRMAN, were interviewed, and these interviews were audio recorded. After being advised that he was not under arrest, GIRMAN indicated he would like to speak with Agents regarding the search warrant and underlying investigation. During GIRMAN's interview, he admitted that he used "cjbwdc" and "cjbusa" to trade pornographic videos, some of which were child pornography, mainly on Kik. GIRMAN also stated that the most recent Kik account that he used to trade child pornography was "chelsbbbb". GIRMAN informed law enforcement that he had lived with Will Smith in Ashburn, VA and that he utilized Smith's WiFi network while residing there.

22. None of the other residents had any knowledge of the circumstances involved with this investigation.

23. A black iPhone, model A1660, with IMEI 355342081245513 was seized and analyzed pursuant to the search warrant. The last activation time of the phone was July 22, 2018. The user accounts installed on the phone included the email address "coreygirman@yahoo.com" and Kik account "chelsbbbb".

24. Hundreds of Kik messages were found on GIRMAN's phone. Consistent with what GIRMAN told law enforcement, GIRMAN used the Kik account "chelsbbbb" in order to print and publish notices seeking and offering to receive, exchange, display and distribute child pornography. For example, on September 5, 2018, GIRMAN sent a Kik message to another individual ("Individual A") which stated, "Any vids of just really young? Giving bjs?" and asking Individual A, "You in any groups?" In another exchange on September 7, 2018, GIRMAN engaged in a Kik message exchange with another individual ("Individual B"). During this exchange, Individual B asked GIRMAN, "Hey, still have your group trade?" GIRMAN, responded, "Yep. Send 2 links." As the exchange ensued, Individual B sent GIRMAN a link to a Dropbox account, indicating that he had "more". GIRMAN responded, "Younger?"

25. In addition to the Kik messages, thousands of thumbnail images were located in the cache of GIRMAN's cellular telephone that depict child pornography. The location of the files is consistent with having viewed, but not stored, the image files. Examples of these images include:

- a. An image file titled "2aAQFIyZ" depicting a prepubescent female child

approximately three to five years old performing oral sex on an adult male.

This image file depicts a child victim whose identity is known to law enforcement.

- b. An image file titled “2bB1zQRb” depicting an adult male inserting his penis into the anus of a prepubescent male child, whose genitalia is also visible. This image file depicts a child victim whose identity is known to law enforcement.
- c. An image file titled “3SQTHARJ” depicting a female toddler lying on a bed on her back. She is covered from the ribcage up with a blanket. She is bound with ropes at the ankles forcing her legs to be spread apart exposing her vagina to the camera. The focus of this image is the lower half of the toddler’s body, to include her vagina and the bindings.

26. Law enforcement has learned that, presently, GIRMAN is in St. Maarten. He is scheduled to fly back to the United States on American Airlines Flight No 2478, and land at the Charlotte/Douglas International Airport at 6:50 p.m. on January 11, 2020. Law enforcement is seeking this warrant to seize and search any Devices that GIRMAN has in his possession when he arrives at the Charlotte/Douglas International Airport.

TECHNICAL TERMS

27. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Digital device,” as used herein, includes the following three terms and their respective definitions:

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. See 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables

and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

c. Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 149.101.1.32). Every computer attached to the internet must be assigned an IP address so that internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. The “internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

e. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers, including access to the internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the internet by using his or her account name and password.

f. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

g. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this Application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Devices, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Device for at least the following reasons:

29. Individuals who engage in criminal activity, including 18 U.S.C. § 2252(a)(1) and (2) (Transportation/Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2251(d)(1)(A) use digital devices for a variety of reasons, including to search for, access, download, view, save, store, back-up and transfer/transport/distribute child exploitative material - including images and videos. Sometimes, digital devices, including cellular telephones, are used to store communications with others involved in the production, sharing, transporting, and distributing of Child Pornography – as GIRMAN has done for a lengthy time period, as detailed above. Digital devices, including cellular telephones, in these types of investigations, often store other evidence of child exploitative material and violations of the law, including logs of online chats, web-browsing history, email correspondence, text or other Short Message Service (SMS) messages, messages using a variety of applications, including Kik as GIRMAN has done in the past. Such

devices may also contain contact information including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts of co-conspirators, and the target of the investigation, as well as images in any form showing underage females and males exposing their genitalia and/or engaged in sexual acts. As stated above, GIRMAN has carried out the majority of his criminal conduct using digital devices, including primarily, a cellular telephone.

30. Based on my training and experience, I know that digital devices are popular due to their small size and mobility. I know that digital devices, including laptop computers, smart phones, and various data storage devices, are commonly transported with their users when they are traveling from place to place. This includes mobile devices, particularly cellular telephones, being transported in and out of the country when the user travels. Such items are commonly recovered from the individual's person during the execution of search warrants.

31. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data. They may use portable laptop computers or digital storage devices to do so. As such, there is reason to believe that any digital device found on GIRMAN in the Charlotte airport could be a facility he used in the commission of his criminal offenses.

32. Digital files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed. Electronic files downloaded to a storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone,

or a storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. As detailed above, this is how images and videos depicting the sexual abuse of children were found on a cellular telephone belonging to GIRMAN. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. The ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

33. As further described in Attachment B, this Application seeks permission to search, locate and seize not only electronic evidence or information that might serve as direct evidence of the crimes described in this Affidavit, but also for forensic electronic evidence or information that establishes how the digital devices were used, the purpose of the use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in the Devices at issue here because:

- a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices including data storage devices

can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device is, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device, not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

- b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.
- c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

34. I know that when an individual uses a digital device to access websites to view child exploitative material, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

35. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

36. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether,

for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

37. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

38. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software

requires specialized tools and a controlled laboratory environment, and can require substantial time.

39. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of

time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

40. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

41. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected

time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your Affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

42. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this Search Warrant will employ the following procedures:

43. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

44. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

45. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

46. Because forensic examiners will be conducting their search of the digital device in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

47. Based on all the reasons described above, I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 US Code § 2252(a)(2) Conspiracy to Receive and Distribute Child Pornography and 18 US Code § 2251(d)(1)(A) Notice Seeking to Receive Child Pornography, and possibly 18 USC 2252(a)(2) Transportation of Child Pornography, as described above and in Attachment B of this Affidavit, may be located on digital devices in the possession of Corey GIRMAN at the time he arrives at the Charlotte/Douglas International Airport I, therefore, respectfully request the attached warrant be issued authorizing the search of any digital devices for the seizure and search of the items listed in Attachment B.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Adam P. Jones", written over a horizontal line.

Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 10, 2020

A handwritten signature in black ink, appearing to read "D. Cayer", written over a horizontal line.

THE HONORABLE DAVID S. CAYER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to any digital devices found on Corey Girman at the time he arrives at the Charlotte/Douglas International Airport.

ATTACHMENT B

Property to be seized

1. The items, information, and data to be seized are fruits, evidence, information relating to, contraband, or instrumentalities, in whatever form and however stored, relating to of violations of 18 U.S.C. §§ 2252(a)(2) and 2251(a)(d)(1) as described in the Search Warrant Affidavit, including, but not limited to:

- a. Child pornography;
- b. Child erotica and evidence of access to children;
- c. Visual depictions of minors engaged in sexually explicit conduct;
- d. Records and information that constitute evidence of the state of mind COREY GIRMAN, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;
- e. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with COREY GIRMAN about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
- f. Evidence of who used, owned, or controlled the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

- g. Evidence of software, or the lack thereof, that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- h. Evidence of the attachment of the Devices to other digital devices;
- i. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Devices;
- j. Evidence of the times the Devices were used;
- k. Passwords, encryption keys, and other access devices that may be necessary to access the Device;
- l. Documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

